CERTIFICATE OF ELECTRONIC TRANSMISSION
I hereby certify that this correspondence is being electronically transmitted to United States Patent and Trademark Office on 09 October 2007.
/Kathryn Marley/
Kathryn Marley

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of inventor: **Len L. Mizrah**	Group Art Unit: **3694**
Application No. **09/706,370**	Examiner: **Ella Colbert**
Confirmation No. **6463**	
Filing Date: **03 November 2000**	**CUSTOMER NO. 22470**
Title: **System and Method for Private and Secure Financial Transactions**	

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is filed in support of appellant's appeal from the fifth Office Action in this case mailed on 21 August 2007. A Notice of Appeal was submitted on 09 October 2007.

The appropriate fee as set forth in § 41.20 (b)(2) of $250.00 for a small entity is included in this submission. Should it be determined that additional fees are required, the Commissioner is hereby authorized to charge those fees to Deposit Account No. 50-0869 (AIDT 1000-1).

///

TABLE OF CONTENTS

TABLE OF AUTHORITIES

There are no authorities cited.

///

REAL PARTY IN INTEREST

The real party in interest is Authernative, Inc., the assignee of record.

RELATED APPEALS AND INTERFERENCES

Applicant is unaware of any related appeals or interferences.

STATUS OF CLAIMS

Claims 1-44, 54, 56 and 57 are canceled. Claims 45-53 and 55 are rejected. Claims 58-82 are withdrawn. The rejections of claims 45-53 and 55 are being appealed. Claims 58-82 were first subjected to a restriction requirement in the office action which is being appealed. Applicant's position is that these claims are a species of the claims being prosecuted and will be subject to rejoinder after a successful appeal.

STATUS OF AMENDMENTS

All requested amendments have been entered. Some claims stand amended and others are in their original form, as indicated in the claims appendix.

SUMMARY OF CLAIMED SUBJECT MATTER

Claim 45 is the sole independent claim. Claims 45, 46, 47, 49, 51, 53 and 55 are separately argued. The remaining claims stand or fall with the claims from which they depend.

In understanding the present invention, it is useful to carefully distinguish between authentication and authorization. Authentication is a process for deciding with confidence that the person seeking to execute a transaction is in fact who he claims to be. Authorization is the process for deciding, given that the person seeking to execute a transaction is in fact who they claim to be, whether that person is acting within his rights under the arrangement with the financial institution.

In the existing credit card infrastructure, authentication is entirely on the merchant, and depends on the merchant obtaining personal identification information from the credit card holder.

The invention removes the step of authentication from the merchant, and makes it the responsibility of the financial institution. The invention includes is an authentication process executed with the financial institution, without merchant involvement, which results in delivery of a transaction signature to the account holder. All the merchant does in the claimed process is identify the transaction, and forward a presented transaction signature to the financial institution.

Given this basic point, the present invention can be characterized as providing a computer-implemented transaction processing method that addresses at least three problems of prior art financial transaction systems. First, the present invention provides a protocol for preventing fraud. Second, the present invention provides a protocol to protect account holder privacy. Third, the present invention provides an architecture that is scalable for implementations handling large numbers of concurrent transactions.

The problem of fraud:

According to the prior art including Tetro (and Watson and Anderson et al. from earlier OA's), computer-driven transactions in which a financial institution server authorizes a transaction with a vendor omit authentication of the account holder, and instead rely upon the vendor to authenticate the account holder. Thus, the vendor obtains both the account number and personal identification information about the account holder. The possession by the vendor of this information about the account holder creates a security loophole and engenders fraud. As is well known, a person having an account number and personal identification information about the account holder can easily execute fraudulent transactions. In the system of the present invention, the techniques and protocols are provided for execution of transactions for which the account number and personal identification information about the account holder are not sufficient for obtaining an authorized transaction. The present invention provides a data processing system which makes access to the account number and personal identification information insufficient to conduct a fraudulent transaction, using technological authentication, authorization and accounting. So even if this information is somehow stolen, it cannot be fraudulently used in the system claimed herein.

The problem of privacy:

Also according to the prior art including Tetro (and Watson and Anderson et al. form earlier OA's), credit and debit card transactions require that the card holder provide personal identity information to the vendor, including personal identification credentials such as name, address, signature and sometimes identification numbers like a driver's license number and social security numbers. Thus, the vendor gains possession of the data that compromises the privacy of the transaction. The vendor also obtains information about the account holder which the account holder may not want to be publicly known. The present invention provides a data processing method which closes this privacy loophole of the prior art, using technological authentication, authorization and accounting that make disclosure of personal identification information to the vendor unnecessary.

The problem of scalability:

The present invention also provides a scalable data processing system architecture, based on the creation and processing of authentication and authorization records, that is capable of efficiently handling large numbers of transactions occurring randomly in time. There is no similar architecture presented in the prior art.

Claim 45

Claim 45 presents a computer implemented method for server-side execution in support of financial transactions. Two records are established during an authorization process and compared, resulting in an authorization if the second is authentic. This method begins with establishing an **authentication** record (510, 907) in memory accessible by server-side computer resources, in response to communications at a first time from a particular account holder, for a predicted transaction by the particular account holder. The first time is a time before a second time, referenced below. The authentication record for the predicted transaction includes [1] a **predicted** transaction amount (W/D), [2] a transaction time parameter (TX1), and [3] an **authenticated transaction signature** (511) **for presentation upon execution of the predicted transaction**. A message including the authenticated transaction signature is sent from the server-side computer resources to the particular account holder.

The method continues with establishing an **authorization** record (906) in memory accessible by server-side computer resources, in response to communications (704) at a second time from a party to a particular transaction. The authorization record for the particular transaction indicates [1] an **actual** transaction amount (709), [2] an actual transaction time (TX2) and [3] a **presented transaction signature** (706). Establishing this second authorization record for the particular transaction does not require identification of the particular account holder.

The method further continues with reading and processing the **authorization** record (906) and the **authentication** record (907) in the server-side computer resources. If the presented transaction signature (706) in the authorization record matches the authenticated transaction signature (511, 703) in the authentication record for the predicted transaction, the actual transaction amount (709) in the authorization record matches the predicted transaction amount (W/D, 707) in the authentication record and the actual transaction time (TX2) in the authorization record matches the transaction time parameter (TX1, 901) in the authentication record, then sending an authorization message (306) to the party of the particular transaction.

The method also includes performing an accounting process (307, 707) that includes reconciling the **predicted** transaction amount and the **actual** transaction amount in the server-side computer resources, for the particular account holder.

Claim 46

Claim 46 builds upon claim 45, extending the method to include storing the **authentication** record (907) in a database including a plurality of authentication records for other predicted transactions.

Claim 47

Claim 47 also builds upon claim 45, specifying for the method that the **time parameter** (TX1, 901) comprises a time value indicating the first time, when the authorization record was created. One can imagine this time stamp embodiment of a time parameter being combined with a system wide or account specific limit on how long the authentication record and transaction signature remain valid, as suggested by claim 48.

Claim 49

Claim 49 also builds upon claim 45, specifying details of establishing the **authentication** record (907). The method includes interacting with a user and producing a transaction signature. The detailed actions include establishing a communication session with the particular account holder, accepting an **account number** and an **identification number** for the particular account holder via the communication session, and accepting the **predicted** transaction amount via the communication session. After this interaction, the method includes producing the transaction signature.

Claim 51

Parallel to claim 49, claim 51 builds upon claim 45, specifying details of interacting with a user to establish the **authorization** record (906). The detailed actions include establishing a communication session with the party to the particular transaction and accepting the **presented transaction signature** and the **actual transaction amount** via the communication session.

Claim 53

Claim 53 builds upon claim 45, extending the method to include maintaining a **list of authorized parties**, and including determining whether the identification of the party accepted via the communication session indicates a party in the list of authorized parties.

Claim 55

Claim 55 also builds upon claim 45, specifying alternative details of establishing an **authentication** record (907). (Compare claim 49.) The method includes interacting with a user in a challenge and response mode to elicit a **dynamically identified combination of digits** from a personal identification code and producing a transaction signature. The detailed actions include establishing a communication session with the particular account holder, accepting an account number via the communication session, prompting the particular account holder via the communication session to supply a static identification number and a **dynamically identified combination of digits** from a personal identification code, wherein the combination does **not** include all of the personal identification code. In these words, the dynamically identified

combination of digits is different from the familiar, static request for the last four digits of a social security number.

The method further includes accepting the **predicted** transaction amount via the communication session, producing the **transaction signature** and sending the transaction signature to the particular account holder.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claim 45 stands rejected under 35 U.S.C. § 112, second paragraph, as being indefinite.

Claims 45-48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over (US 6,095,413) Tetro et al, hereafter Tetro and Official Notice.

Claims 49-53 and 55 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Tetro and Official Notice further in view of (US 6,047,270) Joao et al, hereafter Joao.

///

ARGUMENT

A. Procedural Background

The claims in this appeal are not finally rejected. Nonetheless, the rules permit an appeal in a case, "any of whose claims have been twice rejected." *Ex parte Lemoine*, 46 U.S.P.Q.2D (BNA) 1420 (BPAI 1994) *expanded panel, per curiam*; 35 U.S.C. § 134.

Over the last three years of prosecution, there have been many non-final rejections and no need for an RCE. One final rejection on August 15, 2006 was overcome without an RCE.

The appealed Office Action (AOA) was mailed August 21, 2007.

B. The Examiner Erred in Rejecting Claim 45 Under 35 U.S.C. § 112, Second Paragraph, as being Indefinite, Because "First Time" and "Second Time" are Sufficiently Definite.

After three years of examination, the Examiner urges for the first time in the AOA at 3-4 that phrases using "first time" and "second time" in claim 45, lines 4 and 11 does not make sense and therefore the phrases are vague and indefinite.

The Examiner substantively examined claim 45 and these phrases several times (*e.g.,* OA mailed May 7, 2007) before becoming confused. No explanation is given for the onset of confusion.

The wording of claim 45 makes sense, therefore the phrases identified are not vague or indefinite and the rejection should be reversed. In claim 45, an **authentication** record (907) is established in response to communications at a **first time** with an account holder, who is obtaining pre-authorization **authenticated transaction signature**. An **authorization** record (906) is established at a **second time**, to be compared to the **authentication** record that had been established at the first time.

For example, "the first time" is the time at which an account holder applies to the bank to authenticate a transaction and to obtain a transaction signature in advance of the transaction, and "the second time" is a time after the account holder applies online or offline to a merchant to complete the transaction by submitting the transaction signature, when one of the parties to the transaction communicates with the bank for authorization. The bank creates the authorization record on the back end (the bank's back office) at "the second time", and compares it to the

authentication record to produce the authorization decision and completes the accounting stage of the transaction.

Labels such as "first time" and "second time" are common in patent claims and easily understood. Therefore, the § 112 rejection should be reversed.

C. The Examiner Erred in Rejecting Claims 45-48 Under 35 U.S.C. § 103(a) Because These Claims do Not Read On a Challenge-Response Request for a User's Social Security Number.

1. The Examiner Erred in Rejecting Claim 45

The Examiner's primary reference, Tetro teaches establishing a social security number information database 18 at a first time and prompting a user at a remote terminal 14 to input the user's credit card information, billing address, and social security number at a second time, when making a purchase. Col. 4, lines 21-22 and 33-40. This approach is known as challenge-response. The amount of address information requested may be varied according to the level of security desired. Col. 4, lines 46-48.

The Examiner's argument is styled (AOA at 4-6) as a recitation of the limitations of claim 45 interspersed with occasional parenthetical notes that refer to passages from Tetro, such as "(col. 1, lines 1-40, col. 4, lines 1-59, and col. 7, lines 9-19)" and "(col. 1, lines 1-40, col. 4, lines 16-59, col. 5, lines 54-60, and col. 7, lines 9-1 9)". No guidance is given by the Examiner as to how the passages relate to the claim limitations, other than the positioning of the parentheticals.

None of the passages cited by the Examiner read on any of the limitations of claim 45, when the claim is read as a whole. Tetro does not establish an authentication record, does not generate an authenticated transaction signature, does not use an authenticated transaction signature to authenticate the purchase, and does not combine the authenticated transaction signature with other transaction parameters to determine whether to authorize the transaction. None of these elements are met by Tetro.

We positively claim establishing an authenticated transaction signature (511) for presentation upon execution of a predicted transaction that has a predicted transaction amount. Our authenticated transaction signature does not read on storing an account holder's social

security number. As a corollary, Tetro's social security information database 18, which is established at a first time, does **not** include a predicted transaction amount **or** a transaction time parameter **or** an authenticated transaction signature, so the data record that Tetro establishes at a first time does not read on establishing an **authentication** record that includes all three of these elements.

We further claim establishing an **authorization** record at a second time, when a purchase is being made, including authentication of the user based on a presented transaction signature, **without need to personally identify the account holder**. Authentication of a user based on an authenticated transaction signature (511), without the user's name / telephone number / zip code / etc. is contrary to Tetro's teachings that the user identifies herself and that the level of security may be proportional to the amount of address information requested. Col. 4, lines 21-22 and 33-40. Extending the discussion above, receiving a social security number from a card holder does not read on receiving an authenticated transaction signature (511). The social security number is not part of an authorization record that includes a predicted transaction amount and a transaction time parameter, it is a static bit of information like a zip code or last name. The social security number can not be used to access an authentication record for a transaction with a predicted transaction amount and a transaction time parameter. What Tetro elicits through the vendor at a second time does not read on establishing an **authorization** record, as the elements of an **authorization** record are positively claimed. Tetro's teaches away from our **authorization** record element, because Tetro requires identification of the particular account holder.

Tetro does not read on determining authorization for a transaction by processing the authorization record (906) and the authentication record (907) to determine whether there are matches between [1] the **presented** transaction signature (706) and the **authenticated** transaction signature (511, 703), [2] the **actual** transaction amount (709) and the **predicted** transaction amount (W/D, 707), and [3] the **actual** transaction time (TX2) and the **transaction time parameter** (TX1, 901) in the authentication record. Because claim 45 positively recites details of the comparison used to determine authorization for a particular transaction, Tetro does not read on the authorization process in this third claim element.

Tetro is not even close to reading on claim 45. Therefore, the rejection should be reversed.

For completeness, we respond to the so-called "official notice." (AOA at 6) The Examiner's "official notice" should have been presented as an inherency argument, not official notice. The Examiner wrote, "Official notice is taken that it is well known to read a document prior to processing the document. It would have been obvious to one having ordinary skill in the art at the time the invention was made to first read the record and then process the record and then to authenticate the record if the record matches the required criteria." If all the Examiner is taking notice of is that reading a document is one way to prepare a document for processing, that is true. Here, the official notice is out of place because the document that the Examiner would officially notice being read does not exist. There is no **authentication** record in Tetro's social security database 18, at least as **authentication** record is positively claimed. Applicant specifically challenges and objects to the use of official notice in the rejection, at this first opportunity to do so. We ask the Board to rule that the official notice is improperly taken, not relevant to the rejection and not admissible even under the relaxed evidentiary standards of the Administrative Procedures Act.

Claim 45 and the claims that depend from it should be passed to allowance, as repeated rejections on a variety of art references have been overcome. No further supplemental search should be required at this late stage of prosecution.

2. The Examiner Erred in Rejecting Claim 46

Claim 46 adds to 45 the limitation, "storing the authentication record in a database including a plurality of authentication records for other predicted transactions." The Examiner relies on Tetro at col. 4, line 60 - col. 5, line 18. (AOA at 6), which we reproduce below:

> In order to confirm that valid credit card information has been provided by the user, the input credit card information is submitted an issuer of the user's credit card in step **206**. The issuer possesses a database **16** containing information relating to the credit card accounts for each of its issued credit cards, such as the credit card numbers, expiration dates, billing addresses, and credit limits of its cardholders. A comparison is made between the input credit card information and the stored credit card information in cardholder information database **16** to ensure the input credit card information corresponds to a valid account authorized for the particular transaction being sought. This comparison may be performed either directly by the issuer or by CPU **20** if the cardholder information is communicated back from the issuer to central station **12**. If a valid credit card number has not been input by the user, the electronic credit card information corresponds to a credit card account in the cardholder information database **16**, then the billing address input by the user is compared with a billing address stored in association with the credit card account in cardholder information database **16** in step **210**. The credit card transaction is denied in step **208** if the address input by the user fails to correspond to the stored address, whereas the credit card is authorized by the issuer for the transaction when the input and stored addresses correspond.

is a conventional credit card information database distinct from the social security number database 18. See. col. 6, lines 13-16. In this claim, the antecedent basis for "the authentication record" is found in claim 45 and "includes a predicted transaction amount, a transaction time

parameter, and an authenticated transaction signature." The cardholder information database 16 does not contain a plurality of authentication records as positively claimed.

Applicant respectfully requests that the Honorable Board reverse the rejection and order this claim passed to allowance.

3. The Examiner Erred in Rejecting Claim 47

Claim 47 adds to 45 a time stamp limitation, "wherein the time parameter comprises a time value indicating the first time, when the authorization record was created." The Examiner relies on Tetro at col. 5, lines 19-43. (AOA at 6) The passage relied upon includes both validating credit card information (col. 5, lines 19-20) and comparing both social security information and address information to the social security database 18. The passage relied upon has nothing to do with the time stamp limitation added by claim 47.

As the Examiner's rejection does not make out a *prima facie* case, Applicant urges that it should be reversed.

D. The Examiner Erred in Rejecting Claims 49-53 and 55 Under 35 U.S.C. § 103(a) Because the Interaction Flows are Different.

1. The Examiner Erred in Rejecting Claim 49

Claim 49 describes an interaction between the account holder and the authentication system that establishes an authenticated transaction signature without any involvement of the vendor, which can be presented to a vendor for authentication without identification of the account holder to the vendor. In contrast, Tetro describes an authentication process at the time when the user is "attempting to conduct an electronic credit card transaction." Col. 3, lines 2-4; col. 4, lines 33-35.

The positively claimed actions detail an interaction leading to production of an authenticated transaction signature, which claim 45 teaches is stored in the authentication record and provided to the account holder for presentation to the vendor. In response to the claimed limitations, the Examiner asserts Joao col. 61, lines 54-67, col. 63, lines 5-29, col. 67, line 39 – col. 68, line 19, col 6, lines 40-52 and FIG. 20 (ref 750). (AOA at 7) None of these passages teach an interaction with an account holder leading to generation of an authenticated transaction

signature that can be provided to a merchant as an authentication credential, without identifying the account holder.

Joao does not teach generating an authenticated transaction signature associated with a predicted transaction amount and a time parameter. Joao's basic approach is for the cardholder to identify themselves to a vendor and then have the system use a second message channel to notify and/or challenge the account holder to respond. In some embodiments, Joao teaches starting a credit card transaction and exchanging messages with a two way pager (or text messaging cell phone) to confirm the transaction. In other embodiments, the transaction proceeds and the second message channel is used to notify the account holder so that the account holder can detect and report fraud. None of Joao's teachings, in the context of that invention as a whole, have anything to do with claim 49.

The particular passages relied on by the Examiner do not read on claim 49, in the context of the invention as a whole. The passage at col. 61, lines 54-67 is part of the description of FIG. 20. Joao explains that FIG. 20 includes a transaction device 702 (line 39) and a communications device 704 (line 55). Throughout Joao's embodiments, the transaction device is numbered _ _2 and it is where the transaction is taking place. The second message channel is numbered _ _4 and is where notice or supplemental interaction with the account holder takes place. What Joao teaches at col. 61, lines 54-67 is using e-mail or some other "on-line service" (line 65) as the second message channel. This does not read on claim 49 or an interaction before contacting the vendor that generates an authenticated transaction signature that can be used to authenticate an account holder without identifying the account holder.

The passage at col. 63, lines 5-29, does not teach anything specific, instead reciting that the user can utilize "the present invention to its fullest capabilities over an on-line service … to monitor the operation of the apparatus." It is not clear what this means, but it does not read on claim 49 or an interaction before contacting the vendor that generates an authenticated transaction signature that can be used to authenticate an account holder without identifying the account holder.

The passage at col. 67, line 39 – col. 68, line 19, is closer than the rest, at least to the extent that it suggests that the cardholder should be able to use whatever medium (presumably including on-line message channels, though they are not mentioned in this passage) to temporarily decrease (line 54) or temporarily increase (line 60) their credit limit. The increased

credit limit may be programmed to revert to the reduced credit limit after a major purchase is made (lines 61-64). However, there is no teaching to make the credit limit adjustment part of an authentication record that includes an authenticated transaction record. This passage does not read on claim 49 or an interaction before contacting the vendor that generates an authenticated transaction signature that can be used to authenticate an account holder without identifying the account holder.

The passage at col. 6, lines 40-52 relates to using the second message channel to respond to notices of transactions. The "unauthorized transaction count" in this passage is explained in col. 19, line 35 et seq. The variable "UNAUTHCT" keeps track of the number of times that the second message channel is used for notifications to the account holder without receiving an acknowledgement from the account holder. A limit can be predefined by the system (line 43) or set by the user (col. 20, line 10-12). The technology described in col. 6 and col. 19 does not read on claim 49 or an interaction before contacting the vendor that generates an authenticated transaction signature that can be used to authenticate an account holder without identifying the account holder.

Having looked at each of the passages that the Examiner cited (without any correlating remarks) and found that they do not read on claim 49, Applicant urges that the rejection should be reversed.

2. The Examiner Erred in Rejecting Claim 51

Paralleling claim 49, but for the vendor – authorization center interaction, claim 51 describes an interaction between a party (not the account holder) and the authentication system that includes establishing a communication system and accepting both the presented transaction signature (for comparison to the authenticated transaction signature previously generated) and the transaction amount.

The Examiner responds to claim 51 by citing the same passages from Joao that we traversed above (again without any correlating remarks.) Having looked at each of the passages that the Examiner cited (without any correlating remarks) and found that they do not read on accepting a presented authentication signature for comparison with an authenticated transaction signature, Applicant urges that the rejection should be reversed.

3. The Examiner Erred in Rejecting Claim 55

Claim 55 provides an alternative interaction between the account holder and the authentication system that establishes an authenticated transaction signature without any involvement of the vendor, which can be presented to a vendor for authentication without identification of the account holder to the vendor. This interaction involves a challenge and response for the user to supply "a dynamically identified combination of digits from a personal identification code, wherein the combination does not include all of the personal identification code" as part of the process leading to generation of an authenticated transaction signature. This interaction does not read on consistently requesting the last four digits of a social security number, because the combination of digits is dynamically (as opposed to statically) identified.

The Examiner responds to claim 55 by citing col. 6, line 53 – col. 7, line 55. This passage immediately follows the UNAUTHCT passage from col. 6 that we explained above with reference to col. 19. In cols. 6-7, Joao teaches what notice should be given to an account holder via the second message channel. This passage discusses both the use of the UNAUTHCT variable and effectively setting the variable to zero, requiring acknowledgement from the user via the second message channel within a predetermined time limit.

As discussed above, the technology described in cols. 6-7 and col. 19 does not read on claim 55 or an interaction before contacting the vendor that generates an authenticated transaction signature that can be used to authenticate an account holder without identifying the account holder. Therefore, Applicant urges that the rejection should be reversed.

CONCLUSION

This Application has been thoroughly prosecuted. The examiner's grounds of rejection have been repeatedly overcome. This appeal should result in allowance of the claims without further additional supplemental searches.

It is submitted that all claims subject of this appeal are allowable, and reversal of the rejections is respectfully requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (File No. AIDT 1000-1).

Respectfully submitted,

Dated: 09 October 2007

/Mark A. Haynes/
Mark A. Haynes, Reg. No. 30,846
Attorney for Patent Owner

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
Tel. 650.712.0340
Fax 650.712.0263

CLAIMS APPENDIX

45. (previously presented) A computer implemented method for server-side execution in support of financial transactions, comprising:

establishing an authentication record in memory accessible by server-side computer resources, in response to communications at a first time from a particular account holder, for a predicted transaction by the particular account holder, the authentication record for the predicted transaction includes a predicted transaction amount, a transaction time parameter, and an authenticated transaction signature for presentation upon execution of the predicted transaction, and sending a message including the authenticated transaction signature from the server-side computer resources to the particular account holder;

establishing an authorization record in memory accessible by server-side computer resources, in response to communications at a second time from a party to a particular transaction, for the particular transaction indicating an actual transaction amount, an actual transaction time and a presented transaction signature, wherein said establishing an authorization record does not require identification of the particular account holder;

reading and processing the authorization record and the authentication record in the server-side computer resources, and if the presented transaction signature in the authorization record matches the authenticated transaction signature in the authentication record for the predicted transaction, the actual transaction amount in the authorization record matches the predicted transaction amount in the authentication record and the actual transaction time in the authorization record matches the transaction time parameter in the authentication record, then sending an authorization message to the party of the particular transaction; and

performing an accounting process, including reconciling the predicted transaction amount and the actual transaction amount in the server-side computer resources, for the particular account holder.

46. (original) The method of claim 45, including:

storing the authentication record in a database including a plurality of authentication records for other predicted transactions.

47. (previously presented) The method of claim 45, wherein the time parameter comprises a time value indicating the first time, when the authorization record was created.

48. (original) The method of claim 45, wherein said matching includes determining whether the actual transaction time falls within a time interval indicated by the transaction time parameter.

49. (previously presented)The method of claim 45, wherein establishing an authentication record includes:

establishing a communication session with the particular account holder;

accepting an account number and an identification number for the particular account holder via the communication session;

accepting the predicted transaction amount via the communication session; and

producing the transaction signature.

50. (original) The method of claim 49, including prompting the particular account holder to supply a combination of digits from a personal identification code, wherein the combination does not include all of the personal identification code.

51. (previously presented) The method of claim 45, wherein establishing an authorization record includes:

establishing a communication session with the party to the particular transaction; and

accepting the presented transaction signature and the actual transaction amount via the communication session.

52. (previously presented) The method of claim 51, including accepting identification of the party via the communication session.

53. (previously presented) The method of claim 52, including maintaining a list of authorized parties, and including determining whether the identification of the party accepted via the communication session indicates a party in the list of authorized parties.

54. (canceled).

55. (previously presented) The method of claim 45, wherein establishing an authentication record includes:

establishing a communication session with the particular account holder;

accepting an account number via the communication session;

prompting the particular account holder via the communication session to supply a static identification number and a dynamically identified combination of digits from a personal identification code, wherein the combination does not include all of the personal identification code;

accepting the predicted transaction amount via the communication session; and

producing the transaction signature and sending the transaction signature to the particular account holder.

56-57. (canceled).

58. (withdrawn) A method for managing financial transactions using a computer system arranged for communication with remote devices using communication lines, comprising:

performing a plurality of authentication processes in response to initiations of respective sessions with the computer system by data communications from remote devices, for predicted transactions having predicted transaction amounts and predicted transaction time out intervals by particular account holders, the authentication processes respectively characterized by the steps of:

generating in the computer system requests for input for the corresponding predicted transaction, and receiving in the computer responses to the requests for input from one of said remote devices, wherein said responses to the requests include an identifier of the account used for authenticating the account, at least one parameter unique to the account holder for authenticating the account holder and at least two parameters related to the predicted transaction including a transaction specific parameter and a transaction type identifier unique to the account holder used for authenticating the predicted transaction;

storing a first time-stamped record in memory including the identifier of the account, the at least one parameter unique to the account holder, the transaction specific parameter, the transaction type identifier and a time parameter as a part of or as data associated with the first record in memory; and

producing a transaction signature as a function of the identifier of the account, the at least one parameter unique to the account holder, the transaction specific parameter, the transaction type identifier and the time parameter, for presentation upon execution of the predicted transaction upon authenticating the account, the account holder and the predicted transaction using said responses, associating the transaction signature with the first time-stamped record and transmitting the transaction signature to one of said remote devices associated with the particular account holder;

performing, in the computer system, a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions, the authorization process for a particular transaction characterized by the steps of

receiving an account identifier, a presented transaction signature, and an actual transaction amount at an actual transaction time associated with the authorization request for the particular transaction having a transaction type from one of said remote devices;

storing a second time-stamped record in memory for the authorization request for the particular transaction, the record including the received account identifier, the presented transaction signature, the actual transaction amount and the actual transaction time;

processing the second time-stamped record, in response to one of said first time-stamped records with a matching account identifier, to verify that the presented transaction signature matches the transaction signature associated with said one of said first records, the actual transaction amount matches the predicted transaction amount associated with said one of said first time-stamped records, the actual transaction type matches the transaction type associated with said one of said first records and the actual transaction time is within the predicted transaction time out interval; and

transmitting authorization signals upon successful authorization to one of said remote devices associated with said particular transaction; and

performing, in the computer system, a plurality of accounting processes for the respective transactions subject of authorization processes, including reconciling the predicted

transaction amounts and the actual transaction amounts for each transaction of the particular account holders.

59. (withdrawn) The method of claim 58, including:

storing the predicted transaction type identifier, the predicted transaction amount, and the transaction signature for a predicted transaction in a database in said memory.

60. (withdrawn) The method of claim 58, including storing a predicted transaction time out interval parameter in the database.

61. (withdrawn) The method of claim 58, including setting up a time out interval between the authentication process and the authorization process and after creation of a first time-stamped record for a particular account, monitoring the memory to detect creation of a second time-stamped record having a matching account identifier and attempting said authorization process until one of expiration of the time out interval and success of the authorization process.

62. (withdrawn) The method of claim 58, wherein the authentication process is further characterized by executing a process in the computer system prompting the particular account holder via the communication lines to supply to the computer system a transaction specific code based on or equal to a combination of alphanumeric characters at certain randomly chosen alphanumeric character positions in a password, wherein the combination does not include all of the alphanumeric characters in the password.

63. (withdrawn) The method of claim 58, wherein the authorization process includes:

at the server, performing a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions characterized by prioritizing pairs of first time-stamped records and second time-stamped records with matching account identifiers according to their time stamps and time out interval parameters.

64. (withdrawn) The method of claim 58, including accepting identification of the party at the server.

65. (withdrawn) The method of claim 58, wherein the authorization process operates without identification of the particular account holder to the party.

66. (withdrawn) The method of claim 58, wherein the authorization process operates with identification of the particular account holder to the party.

67. (withdrawn) A financial transaction server, comprising:

a communication interface;

a computer system including memory coupled to the communication interface, the data processing system including resources for managing financial transactions and for communicating using the communication interface with remote devices, including

an authentication process communicating over the communication interface for authenticating a predicted transaction by a particular account holder, including routines characterized by the steps of:

generating in the computer system requests for input for the corresponding predicted transaction, and receiving in the computer responses to the requests for input from one of said remote devices, wherein said responses to the requests include an identifier of the account used for authenticating the account, at least one parameter unique to the account holder for authenticating the account holder and at least two parameters related to the predicted transaction including a transaction specific parameter and a transaction type identifier unique to the account holder used for authenticating the predicted transaction;

storing a first time-stamped record in memory including the identifier of the account, at least one parameter unique to the account holder for authenticating the account holder, the transaction specific parameter, the transaction type identifier and a time parameter as a part of or as data associated with the first record in memory; and

producing a transaction signature as a function of the identifier of the account, the at least one parameter unique to the account holder, the transaction specific parameter, the transaction type identifier and the time parameter, for presentation upon execution of the predicted

transaction upon authenticating the account, the account holder and the predicted transaction using said responses, associating the transaction signature with the first time-stamped record and transmitting the transaction signature to one of said remote devices associated with the particular account holder;

an authorization process communicating over the communication interface for authorizing a particular transaction having an actual transaction amount and an actual transaction time, including routines characterized by the steps of:

receiving an account identifier, a presented transaction signature, and an actual transaction amount at an actual transaction time associated with the authorization request for the particular transaction having a transaction type from one of said remote devices;

storing a second time-stamped record in memory for the authorization request for the particular transaction, the record including the received account identifier, the presented transaction signature, the actual transaction amount and the actual transaction time;

processing the second time-stamped record, in response to one of said first time-stamped records with a matching account identifier, to verify that the presented transaction signature matches the transaction signature associated with said one of said first records, the actual transaction amount matches the predicted transaction amount associated with said one of said first time-stamped records, the actual transaction type matches the transaction type associated with said one of said first records and the actual transaction time is within the predicted transaction time out interval; and

transmitting authorization signals upon successful authorization to one of said remote devices associated with said particular transaction; and

an accounting process executed in combination with said authorization processes for respective transactions, including reconciling the predicted transaction amounts and the actual transaction amounts for each transaction of the particular account holders.

68. (withdrawn) The financial transaction server of claim 67, wherein the data processing system includes a local or remote database storing the first and second time-stamped records.

69. (withdrawn) The financial transaction server of claim 67, wherein the data processing system includes a watchdog routine which after creation of a first time-stamped record for a

particular account, monitors the memory to detect creation of a second time-stamped record having a matching account identifier and attempts said authorization process until one of expiration of the time out interval and success of the authorization process.

70. (withdrawn) The financial transaction server of claim 67, wherein the authentication process includes routines performing a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions characterized by prioritizing pairs of first time-stamped records and second time-stamped records with matching account identifiers according to their time stamps and time out interval parameters.

71. (withdrawn) The financial transaction server of claim 67, wherein the authentication process includes a routine prompting the particular account holder via the communication interface to supply to the computer system a transaction specific code based on or equal to a combination of alphanumeric characters at certain randomly chosen alphanumeric character positions in a password, wherein the combination does not include all of the alphanumeric characters in the password.

72. (withdrawn) The financial transaction server of claim 67, wherein the authorization process includes a routine accepting identification of the party at the server.

73. (withdrawn) The financial transaction server of claim 67, wherein the authorization process operates without identification of the particular account holder to the party.

74. (withdrawn) The financial transaction server of claim 67, wherein the authorization process operates with identification of the particular account holder to the party.

75. (withdrawn) An article of manufacture, comprising:

a machine readable storage medium;

a computer program stored on said machine readable medium with resources executable by a computer system for managing financial transactions, including

an authentication process communicating over the communication interface for authenticating predicted transaction by a particular account holder, including routines characterized by the steps of:

generating in the computer system requests for input for the corresponding predicted transaction, and receiving in the computer responses to the requests for input from one of said remote devices, wherein said responses to the requests include an identifier of the account used for authenticating the account, at least one parameter unique to the account holder for authenticating the account holder and at least two parameters related to the predicted transaction including a transaction specific parameter and a transaction type identifier unique to the account holder used for authenticating the predicted transaction;

storing a first time-stamped record in memory including the identifier of the account, at least one parameter unique to the account holder for authenticating the account holder, the transaction specific parameter, the transaction type identifier and a time parameter as a part of or as data associated with the first record in memory; and

producing a transaction signature as a function of the identifier of the account, the at least one parameter unique to the account holder, the transaction specific parameter, the transaction type identifier and the time parameter, for presentation upon execution of the predicted transaction upon authenticating the account, the account holder and the predicted transaction using said responses, associating the transaction signature with the first time-stamped record and transmitting the transaction signature to one of said remote devices associated with the particular account holder;

an authorization process communicating over the communication interface for authorizing a particular transaction having an actual transaction amount and an actual transaction time, including routines characterized by the steps of

receiving an account identifier, a presented transaction signature, and an actual transaction amount at an actual transaction time associated with the authorization request for the particular transaction having a transaction type from one of said remote devices;

storing a second time-stamped record in memory for the authorization request for the particular transaction, the record including the received account identifier, the presented transaction signature, the actual transaction amount and the actual transaction time;

processing the second time-stamped record, in response to one of said first time-stamped records with a matching account identifier, to verify that the presented transaction signature matches the transaction signature associated with said one of said first records, the actual transaction amount matches the predicted transaction amount associated with said one of said first time-stamped records, the actual transaction type matches the transaction type associated with said one of said first records and the actual transaction time is within the predicted transaction time out interval; and

transmitting authorization signals upon successful authorization to one of said remote devices associated with said particular transaction; and

an accounting process executed in combination with said authorization processes for the respective transactions, including reconciling the predicted transaction amounts and the actual transaction amounts for each transaction of the particular account holders.

76. (withdrawn) The article of claim 75, wherein the resources include a routine for storing the first and second time-stamped records in a local or remote database.

77. (withdrawn) The article of claim 75, wherein the resources include a watchdog routine which after creation of a first record for a particular account, monitors the memory to detect creation of a second record having a matching account identifier and attempts said authorization process until one of expiration of the time out interval and success of the authorization process.

78. (withdrawn) The article of claim 75, wherein the authentication process includes a routine prompting the particular account holder via the communication interface to supply to the computer system a transaction specific code based on or equal to a combination of alphanumeric characters at certain randomly chosen alphanumeric character positions in a password, wherein the combination does not include all of the alphanumeric characters in the password.

79. (withdrawn) The article of claim 75, wherein the authorization process includes routines performing a plurality of authorization processes for particular transactions in response to authorization requests from parties to actual transactions characterized by prioritizing pairs of

first time-stamped records and second time-stamped records with matching account identifiers according to their time stamps and time out interval parameters

80. (withdrawn) The article of claim 75, wherein the authorization process includes a routine accepting identification of the party at the server.

81. (withdrawn) The article of claim 75, wherein the authorization process operates without identification of the particular account holder to the party.

82. (withdrawn) The article of claim 75, wherein the authorization process operates with identification of the particular account holder to the party.

EVIDENCE APPENDIX

Applicant is not submitting any evidence in this appendix.

RELATED PROCEEDINGS APPENDIX

Applicant is not aware of any related appeals or interferences.